

<b>Module Information</b>	
<b>Module Title</b>	<b>Wired and Wireless Embedded Networks</b>
<b>Module Code</b>	<b>ESD 530</b>

## 1. MODULE SUMMARY

### Aims and Summary

This module intends to prepare the student as an embedded network engineer well-versed with wired and wireless networks along with network security concepts. The students will be taught concepts of wired and wireless protocols as well as serial buses used in embedded network systems; also, knowledge of principles, practices and techniques of network security will be imparted. The students will be trained on the use of commercial software tools for development and simulation of embedded networks.

### Module Size and Credits

<b>Module size</b>	Single
<b>CATS points</b>	12
<b>ECTS credits</b>	N/A
<b>Open / restricted</b>	Restricted
<b>Availability on/off campus</b>	On Campus
<b>Total student study hours</b>	120
<b>Number of weeks</b>	4 weeks Full-time or 8 weeks Part-time.
<b>Centre responsible</b>	Embedded System Design Centre/Department of Electronics and Communication Engineering
<b>Academic Year</b>	2009

### Entry Requirements (pre-requisites and co-requisites)

Normally to be qualified for entry to the Postgraduate Engineering Programme

### Excluded Combinations

None

### Composition of Module Mark (including weighting of components)

Full-time / Part-time : 50% Written Examination and 50 % Assignment

### Pass Requirements

A minimum of 40 % marks in the written examination and a minimum of 40% marks in the assignment are required for a pass and overall 40% marks

### Special Features

80% attendance in theory and 80% attendance in laboratory are required.  
It is likely that considerable time will be spent in School facilities outside of normal timetabled class time.

### Courses for which this module is mandatory

M.Sc. [Engg] in Real Time Embedded Systems

### Courses for which this module is a core option

None

## 2. TEACHING, LEARNING AND ASSESSMENT

### Intended Module Learning Outcomes

After undergoing this module, students will be able to:

1. Analyse and develop embedded network systems using various wired and wireless network protocols
2. Describe network security concepts for embedded network systems
3. Proficiently use commercially available development and simulation tools for embedded networks

### Indicative Content

#### Class Room Lectures

1. **Overview of Network Embedded Systems** - Design constraints, Modular design, OSI layers, TCP and UDP concepts
2. **Inter-Process Communication (IPC) Mechanism** - Concept of sockets, Socket programming, Remote procedure calls and Programming for Client-Server communication over UDP/TCP
3. **Real-time Transport Protocol (RTP)** – RTP, RTCP & related standards, RTP services, Header & packet formats, RTP APIs for Linux environment and Case studies on RTP
4. **Application Layer Protocols** - BOOTP, DHCP, FTP, RLOGIN, SNMP, SMTP, TELNET, Ping, HTTP and HTTPS
5. **Serial Peripheral Interface (SPI) Bus** - Principle, Modes of SPI transfer, Different configurations (such as master-slave, daisy chain), Advantages & disadvantages and Case Study
6. **Controller Area Network (CAN)** – History of CAN, Fundamentals of CAN, Layers in CAN, Description of CAN message formats, Overview of different layers, Typical CAN with two nodes, CAN communication between two different Microcontrollers and Case studies
7. **Local Interconnect Network (LIN)** – Basics concepts of LIN, Communication mechanism and Master-slave configuration
8. **Inter Integrated Circuit (I2C) Protocol** – Basics concepts of I2C, Master-slave & Multi-master concepts with Start & Stop conditions and Case studies
9. **FlexRay Protocol** - Future on board systems, Need for FlexRay, Origin of FlexRay, FlexRay consortium, FlexRay objectives, FlexRay features, Application requirements, Working of FlexRay, Network topologies, ECU architecture, Segment configuration, Communication cycles, FlexRay frame format, Timing of configuration protocol, Error control, FlexRay core mechanisms, Coding, Decoding, Medium access control, Frame & symbol processing, Clock synchronization, FlexRay components, Comparison with other IVN protocols and Case Study
10. **Media Oriented System Transport (MOST) Protocol** – MOST in car systems, MOST goals, Features, Cables & connectors, Data types, Topology, Frame format, Application areas, System description, Specification, Device model, Device implementation, Diagnostics and Case Study
11. **Universal Serial Bus (USB)** – Basics concepts of USB, Study of USB host & devices, Communication using USB, USB connectors and USB cables
12. **Wireless Communication** - Overview of wireless communication systems, ITU-T standards and ISM
13. **Wireless Personal Area Networks (WPANs) Technologies** - Bluetooth, Zigbee, IrDA and Case study
14. **Wireless Local Area Networks (WLANs)** - Introduction to WLANs, Applications of WLAN, WLAN topologies, WLAN MAC and 802.11 standards
15. **Security Basics** – Threats, Vulnerabilities, Security policies, Attack types for network security (sniffing, spoofing, hijacking, denial-of-service), Typical attack process & counter-measures and Security services & mechanisms.
16. **Network Security** - Secret key ciphers, Public key ciphers, Data Encryption Standard (DES), Advanced Encryption Standard (AES), Public key infrastructure, Message authentication, Digital signatures, providing security at different network layers and Case studies.

#### Laboratory Practice

1. Working with embedded microcontrollers/hardware boards – PIC/LPC2129/PXA with related IDEs
2. Socket programming in C for networking using TCP, UDP, and RPC
3. Working with application layer protocols –FTP, telnet, rlogin, Ping.
4. Developing network application in C using RTP
5. Client server program in C using RTP
6. Embedded client server application in C on ARM processors using TCP/IP
7. Embedded chat application on ARM processor/microcontroller

8. Real time clock control using I2C protocol
9. CAN – development of embedded messaging application
10. CAN-I2C gateway
11. MOST and Flexray on CANoe
12. Network security concepts using AES/DES algorithms
13. WLAN Demo
14. Bluetooth using MATLAB/SIMULINK.

### Teaching and Learning Methods

1. Theoretical Knowledge [~30% of module time]
  - a. Face to face lectures from a module leader- 30 hours
  - b. Case study teaching and discussion from a practicing engineer on special topics - 6 hours

**36 hours**
2. Laboratory Practice (Skills) [~ 25% of module time]
 

**30 hours**
3. Application Orientation and Problem Solving [45% of module time]
  - a. Reading
  - b. Research
  - c. Written Examination
  - d. Assignment Solving and Documentation

**54 hours**

### Method of Assessment

#### Part-A

Written Examination [50% Weightage]

At the end of the module, normally on the last day of the last week of the module, written examination is conducted to test students' understanding of taught theoretical concepts. The question paper will comprise either or a combination of the following:

- 6 questions, out of which 5 questions need to be answered
- Practical laboratory work
- Presentations
- Field work
- Creation of a physical model

The marks scored by the student will be scale down to 50% weight.

#### Part –B

Assignment [50% Weightage]

Students are required to submit word processed assignment report on formally announced last day of the module. Assignment tests students' problem solving skills based on taught concepts. The assignment is assessed for 100 marks but scored marks is scaled down to 50%

<b>Assessment</b>			
<b>Learning Outcomes</b>	<b>1</b>	<b>2</b>	<b>3</b>
<b>Part A</b>	<b>X</b>	<b>X</b>	
<b>Part B</b>	<b>X</b>	<b>X</b>	<b>X</b>

Both written examination scripts and assignment reports will be double marked/valued

### Re-assessment

A minimum of 40 % marks in the written examination and a minimum of 40% marks in the assignment are required for a pass in the module.

A student failing in any one of the components or both is considered as FAIL in the module. A failed student is required to retake the module at the next opportunity. A maximum of 3 attempts including the original are allowed.

#### **Date of Last Amendment**

May -2009

### **3. MODULE RESOURCES**

#### **Essential Reading**

1. Module Notes

#### **Recommended Reading**

##### **Books**

1. H. Kopetz, *Real-Time Systems: Design Principles for Distributed Embedded Applications*, Kluwer, 1997
2. William Stallings, *Cryptography and Network Security: Principles and Practice*, 2<sup>nd</sup> edition, Prentice Hall, 1998
3. William Stallings, *Network Security Essentials*, 3<sup>rd</sup> edition, Prentice Hall, 2006
4. Saadat Malik, *Network Security Principles and Practices (CCIE Professional Development)*, Pearson Education, 2002
5. Douglas R. Stinson, *Cryptography: theory and practice*, 2<sup>nd</sup> edition, CRC press, 2002
6. Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2<sup>nd</sup> edition, John Wiley & Sons, 1995
7. Stephen Kochan and Patrick H. Wood, *Unix Networking*, Prentice Hall India, 1989
8. Mukesh Singhal and Niranjana G. Shivaratri, *Advanced Concepts in Operating System*, Tata-McGraw Hill, 2003
9. Theodore Rappaport, *Wireless Communications: Principles and Practice*, 2<sup>nd</sup> edition, Prentice-Hall Publishers, 2001

##### **Journals**

1. International Journal of Network Security
2. ACM Transactions on Information and System Security (TISSEC)
3. IEEE Transactions on Dependable and Secure Computing (TDSC)
4. IEEE Transactions on Information Forensics and Security
5. IEEE Transactions on Communications

##### **Magazines**

1. IEEE Security and Privacy
2. IEEE Communication Magazine

##### **Internet Sites**

1. CAN Specification 2.0, [www.semiconductors.bosch.de/pdf/can2spec.pdf](http://www.semiconductors.bosch.de/pdf/can2spec.pdf)
2. SPI Protocol, <http://www.mct.net/faq/spi.html>
3. Internet Protocol Standards, <http://www.rfc-editor.org/rfcxx00.html>
4. SPI Handbook, <http://www.scribd.com/doc/7342359/SPI-HandBook>
5. Local Interconnect Network, <http://www.lin-subbus.org>
6. Universal Serial Bus, <http://www.usb.org>
7. USB in a NutShell, <http://www.beyondlogic.org/usbnutshell>
8. Intelligent Security Solutions, <http://www.ibm.com/takebackcontrol/in/security>

##### **Laboratory**

**Hardware:** LPC2129, PIC18F448/458, PXA Board, MCP2551, DS1307 RTC

**Software:** Keil Microvision for ARM, MP Lab IDE, Linux Kernel

**Software Manual:** Module Lab manual, LPC2129 user guide, PXA Board manual

#### 4. MODULE ORGANISATION

##### Module Leader

<b>Name</b>	Ramya Bhaskaran
<b>Room</b>	S-19
<b>Telephone number</b>	080-2360 5539-310
<b>E-mail</b>	ramya@msrsas.org

##### Date and Time of Examination

As per time table

##### Subject Quality and Approval Information

<b>Subject Quality Group / Subject Board</b>	Electronics and Communication Engineering
<b>Subject Assessment Board</b>	Postgraduate Engineering Programmes
<b>Shortened title</b>	WNW
<b>Date of approval by MARP</b>	May 2009